Amendments to the Claims

Claim 1 (currently amended): In a computing environment having a plurality of secure network connections ~~connection to a network~~, a computer program product for securely propagating security credentials using a trusted authenticating domain, the computer program product embodied on one or more computer-readable media and comprising:

~~computer-readable program code means for establishing a secure connection between a client and a password synchronization agent (PSA);~~

computer-readable program code means for receiving, ~~at the PSA~~ by a password synchronization agent ("PSA") from a user at a [[the]] client device over [[the]] a first secure connection between the client device and the PSA on which the PSA has authenticated itself to the client device, a password propagation request providing an identifier of [[a]] the user and an identifying secret of the user ~~during propagation request processing~~;

computer-readable program code means for ~~validating the user with the~~ forwarding, by the PSA to a trusted authenticating domain over a second secure connection therebetween on which the trusted authenticating domain has authenticated itself to the PSA, [[using]] the received user identifier and identifying secret, ~~on request of the PSA~~ wherein the trusted authenticating domain stores identifying secrets for user identifiers only as secured, non-recoverable versions thereof;

computer-readable program code means for receiving, by the PSA from the trusted authenticating domain over the second connection, a validation result created by the trusted authenticating domain responsive to the forwarding, the validation result being a successful result if it indicates that the trusted authenticating domain had previously stored, for the user identifier,

a secured version of the identifying secret; and

computer-readable program code means for propagating, if the validation result is the successful result, the received user identifier and identifying secret ~~of the user directly~~ from the PSA to a master registry ~~if the validation succeeds~~ over a third mutually-authenticated secure connection therebetween, such that the master registry can store, for the user identifier, a secured version of the identifying secret, wherein the secured version stored by the master registry is not required to be identical to the secured version stored at the trusted authenticating domain.

Claims 2 - 3 (canceled)

Claim 4 (currently amended): The computer program product according to Claim 1, further comprising computer-readable program code means for propagating, if the validation result is the successful result, the received identifying secret from the PSA to one or more [[other]] target registries over fourth mutually-authenticated secure connections, each of the fourth connections being between the PSA and a distinct one of the target registries, such that each target registry can store, for the user identifier, a secured version of the identifying secret ~~if the validation succeeds~~.

Claim 5 (canceled)

Claim 6 (currently amended): The computer program product according to Claim 1, ~~further comprising:~~

~~computer-readable program code means for obtaining~~ wherein the password propagation request further provides an identification of the trusted authenticating domain ~~from the user during the propagation request processing~~; and

further comprising computer-readable program code means for verifying that the trusted authenticating domain is trusted by the master registry as a prerequisite to the propagating.

Claim 7 (currently amended): The computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining, by the PSA using the third connection, an identification of the trusted authenticating domain from the master registry as a prerequisite to the forwarding.

Claim 8 (currently amended): The computer program product according to Claim 6, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for verifying that the trusted authenticating domain is trusted further comprises computer-readable program code means for checking whether the stored trust policy information for the user identifier includes the trusted authenticating domain identification ~~obtained from the user~~ provided in the password propagation request.

Claim 9 (currently amended): The computer program product according to Claim 6, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for verifying that the trusted authenticating domain is trusted further comprises computer-

readable program code means for checking whether the stored trust policy information for a user group of which the user identified by the user identifier is a member includes the trusted authenticating domain identification ~~obtained from the user~~ provided in the password propagation request.

Claim 10 (currently amended): The computer program product according to Claim 7, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for obtaining the identification of the trusted authenticating domain from the master registry further comprises computer-readable program code means for obtaining the trusted authenticating domain identification using the stored trust policy information for the user identifier.

Claim 11 (currently amended): The computer program product according to Claim 7, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for obtaining the identification of the trusted authenticating domain from the master registry further comprises computer-readable program code means for obtaining the trusted authenticating domain identification using the stored trust policy information for a user group of which the user identified by the user identifier is a member.

Claim 12 (currently amended): The computer program product according to Claim 4, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the received identifying secret to the one

or more [[other]] target registries further comprises computer-readable program code means for identifying the one or more other target registries using the stored password synchronization policy information for the user identifier.

Claim 13 (currently amended): The computer program product according to Claim 4, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the received identifying secret to the one or more [[other]] target registries further comprises computer-readable program code means for identifying the one or more other target registries using the stored password synchronization policy information for a user group of which the user identified by the user identifier is a member.

Claims 14 - 17 (canceled)

Claim 18 (currently amended): The computer program product according to Claim 1, wherein the previously-stored secured version of the identifying secret was created, at the trusted authenticating domain, by ~~computer-readable program code means for validating further comprises:~~

~~computer-readable program code means for~~ performing a security function on a previously-received copy of the ~~received~~ identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

~~computer-readable program code means for using the received user identifier to locate a~~

~~previously-stored identifying secret of the user which was stored by the trusted authenticating domain; and~~

wherein the security function is repeated, at the trusted authenticating domain, on the forwarded identifying secret of the user, after which, if a result thereof is identical to the previously-stored secured version, the trusted authenticating domain then creates the successful result ~~computer-readable program code means for concluding that the validation succeeds if the located identifying secret is identical to a result of performing the security function~~.

Claim 19 (currently amended): The computer program product according to Claim 1, wherein the validation result is created, at the trusted authenticating domain, by ~~computer-readable program code means for validating further comprises computer-readable program code means for~~ invoking an authenticated LDAP bind or other native authentication mechanism of the trusted authenticating domain, ~~wherein the received~~ using the forwarded user identifier ~~of the user~~ and the ~~received~~ identifying secret of the user, and wherein the validation result is created using a result of the LDAP bind or other native authentication mechanism ~~are passed to the trusted authenticating domain, thereby causing the trusted authenticating domain to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation~~.

Claim 20 (original): The computer program product according to Claim 1, wherein the PSA has administrative authority for performing operations at the master registry.

Claim 21 (currently amended): The computer program product according to Claim 4, wherein the PSA has administrative authority for performing operations at the one or more [[other]] target registries.

Claim 22 (currently amended): A system for securely propagating security credentials using a trusted authenticating domain, comprising:

~~means for establishing a secure connection between a client and a password synchronization agent (PSA);~~

means for receiving, ~~at the PSA~~ by a password synchronization agent ("PSA") from a user at a [[the]] client device over [[the]] a first secure connection between the client device and the PSA on which the PSA has authenticated itself to the client device, a password propagation request providing an identifier of [[a]] the user and an identifying secret of the user ~~during propagation request processing;~~

means for ~~validating the user with the~~ forwarding, by the PSA to a trusted authenticating domain over a second secure connection therebetween on which the trusted authenticating domain has authenticated itself to the PSA, [[using]] the received user identifier and identifying secret, ~~on request of the PSA~~ wherein the trusted authenticating domain stores identifying secrets for user identifiers only as secured, non-recoverable versions thereof;

means for receiving, by the PSA from the trusted authenticating domain over the second connection, a validation result created by the trusted authenticating domain responsive to the forwarding, the validation result being a successful result if it indicates that the trusted authenticating domain had previously stored, for the user identifier, a secured version of the

identifying secret; and

means for propagating, if the validation result is the successful result, the received user identifier and identifying secret ~~of the user directly~~ from the PSA to a master registry ~~if the validation succeeds~~ over a third mutually-authenticated secure connection therebetween, such that the master registry can store, for the user identifier, a secured version of the identifying secret, wherein the secured version stored by the master registry is not required to be identical to the secured version stored at the trusted authenticating domain.

Claims 23 - 24 (canceled)

Claim 25 (currently amended): The system according to Claim 22, further comprising means for propagating, if the validation result is the successful result, the received identifying secret from the PSA to one or more [[other]] target registries over fourth mutually-authenticated secure connections, each of the fourth connections being between the PSA and a distinct one of the target registries, such that each target registry can store, for the user identifier, a secured version of the identifying secret ~~if the validation succeeds~~.

Claim 26 (canceled)

Claim 27 (currently amended): The system according to Claim 22, ~~further comprising:~~

~~means for obtaining~~ wherein the password propagation request further provides an identification of the trusted authenticating domain ~~from the user during the propagation request~~

processing; and

further comprising means for verifying that the trusted authenticating domain is trusted by the master registry as a prerequisite to the propagating.

Claim 28 (currently amended): The system according to Claim 22, further comprising:

means for obtaining, by the PSA using the third connection, an identification of the trusted authenticating domain from the master registry as a prerequisite to the forwarding.

Claim 29 (currently amended): The system according to Claim 27, wherein the master registry stores trust policy information, and wherein the means for verifying that the trusted authenticating domain is trusted further comprises means for checking whether the stored trust policy information for the user identifier includes the trusted authenticating domain identification ~~obtained from the user~~ provided in the password propagation request.

Claim 30 (currently amended): The system according to Claim 27, wherein the master registry stores trust policy information, and wherein the means for verifying that the trusted authenticating domain is trusted further comprises means for checking whether the stored trust policy information for a user group of which the user identified by the user identifier is a member includes the trusted authenticating domain identification ~~obtained from the user~~ provided in the password propagation request.

Claim 31 (currently amended): The system according to Claim 28, wherein the master registry

stores trust policy information, and wherein the means for obtaining the identification of the trusted authenticating domain from the master registry further comprises means for obtaining the trusted authenticating domain identification using the stored trust policy information for the user identifier.

Claim 32 (currently amended): The system according to Claim 28, wherein the master registry stores trust policy information, and wherein the means for obtaining the identification of the trusted authenticating domain from the master registry further comprises means for obtaining the trusted authenticating domain identification using the stored trust policy information for a user group of which the user identified by the user identifier is a member.

Claim 33 (currently amended): The system according to Claim 25, wherein the master registry stores password synchronization policy information, and wherein the means for propagating the received identifying secret to the one or more [[other]] target registries further comprises means for identifying the one or more other target registries using the stored password synchronization policy information for the user identifier.

Claim 34 (currently amended): The system according to Claim 25, wherein the master registry stores password synchronization policy information, and wherein the means for propagating the received identifying secret to the one or more other target registries further comprises means for identifying the one or more [[other]] target registries using the stored password synchronization policy information for a user group of which the user identified by the user identifier is a

member.

Claims 35 - 38 (canceled)

Claim 39 (currently amended): The system according to Claim 22, wherein the previously-stored secured version of the identifying secret was created, at the trusted authenticating domain, by ~~means for validating further comprises:~~

~~means for~~ performing a security function on a previously-received copy of the ~~received~~ identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

~~means for using the received user identifier to locate a previously-stored identifying secret of the user which was stored by the trusted authenticating domain;~~ and

wherein the security function is repeated, at the trusted authenticating domain, on the forwarded identifying secret of the user, after which, if a result thereof is identical to the previously-stored secured version, the trusted authenticating domain then creates the successful result ~~means for concluding that the validation succeeds if the located identifying secret is identical to a result of performing the security function.~~

Claim 40 (currently amended): The system according to Claim 22, wherein the validation result is created, at the trusted authenticating domain, by ~~means for validating further comprises means for~~ invoking an authenticated LDAP bind or other native authentication mechanism of the trusted authenticating domain, ~~wherein the received~~ using the forwarded user identifier ~~of the user~~ and

the ~~received~~ identifying secret of the user, and wherein the validation result is created using a result of the LDAP bind or other native authentication mechanism ~~are passed to the trusted authenticating domain, thereby causing the trusted authenticating domain to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation~~.

Claim 41 (original): The system according to Claim 22, wherein the PSA has administrative authority for performing operations at the master registry.

Claim 42 (currently amended): The system according to Claim 25, wherein the PSA has administrative authority for performing operations at the one or more [[other]] target registries.

Claim 43 (currently amended): A computer-implemented method for securely propagating security credentials using a trusted authenticating domain, comprising steps of:

~~establishing a secure connection between a client and a password synchronization agent (PSA);~~

receiving, ~~at the PSA~~ by a password synchronization agent ("PSA") from a user at a [[the]] client device over [[the]] a first secure connection between the client device and the PSA on which the PSA has authenticated itself to the client device, a password propagation request providing an identifier of [[a]] the user and an identifying secret of the user ~~during propagation request processing~~;

~~validating the user with the~~ forwarding, by the PSA to a trusted authenticating domain

over a second secure connection therebetween on which the trusted authenticating domain has authenticated itself to the PSA, [[using]] the received user identifier and identifying secret, ~~on request of the PSA~~ wherein the trusted authenticating domain stores identifying secrets for user identifiers only as secured, non-recoverable versions thereof;

receiving, by the PSA from the trusted authenticating domain over the second connection, a validation result created by the trusted authenticating domain responsive to the forwarding, the validation result being a successful result if it indicates that the trusted authenticating domain had previously stored, for the user identifier, a secured version of the identifying secret; and

propagating, if the validation result is the successful result, the received user identifier and identifying secret ~~of the user directly~~ from the PSA to a master registry ~~if the validation succeeds~~ over a third mutually-authenticated secure connection therebetween, such that the master registry can store, for the user identifier, a secured version of the identifying secret.

Claim 44 (currently amended): The computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining a new value from the user to be used as the propagated identifying secret if the validation ~~succeeds~~ has the successful result; and

computer-readable program code means for substituting [[this]] the new value for the received identifying secret prior to operation of the computer-readable program code means for propagating.

Claim 45 (currently amended): The system according to Claim 22, further comprising:

means for obtaining a new value from the user to be used as the propagated identifying secret if the validation ~~succeeds~~ has the successful result; and

means for substituting [[this]] the new value for the received identifying secret prior to operation of the means for propagating.

Claim 46 (currently amended): The method according to Claim 43, further comprising steps of:

obtaining a new value from the user to be used as the propagated identifying secret if the validation ~~succeeds~~ has the successful result; and

substituting [[this]] the new value for the received identifying secret prior to operation of the propagating step.

Claim 47 (new): The method according to Claim 43, wherein the forwarding and receiving steps use secure interprocess communications between the PSA and the trusted authenticating domain instead of the second connection.

Claim 48 (new): The method according to Claim 43, wherein the secured version stored by the master registry is not required to be identical to the secured version stored at the trusted authenticating domain.